UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/541,215	06/30/2005	Shinji Hamai	2005_1027A	4866

513   7590   11/18/2008
WENDEROTH, LIND & PONACK, L.L.P.
2033 K STREET N. W.
SUITE 800
WASHINGTON, DC 20006-1021

EXAMINER
POPHAM, JEFFREY D

ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
11/18/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _12 August 2008_.
2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.
3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1,3-8 and 11-17_ is/are pending in the application.
    4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5)☐ Claim(s) _____ is/are allowed.
6)☒ Claim(s) _1,3-8 and 11-17_ is/are rejected.
7)☐ Claim(s) _____ is/are objected to.
8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.
10)☒ The drawing(s) filed on _30 June 2005_ is/are: a)☒ accepted or b)☐ objected to by the Examiner.
    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
    a)☒ All   b)☐ Some * c)☐ None of:
      1.☒ Certified copies of the priority documents have been received.
      2.☐ Certified copies of the priority documents have been received in Application No. _____.
      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Remarks

Claims 1, 3-8, and 11-17 are pending.

Response to Arguments

1.   Applicant's arguments filed 8/12/2008 have been fully considered but they are not persuasive.

Regarding the information disclosure statements, the Examiner still does not find copies of each non-patent literature publication within the file.

Applicant argues that Naor teaches that a newly received certificate is compared with every certificate contained in the CRL, but does not teach use of identification numbers being greater than or equal to a revocation number as providing certificate validity while identification numbers less than the revocation number are invalid. Applicant discusses how Naor states that there is a high cost associated with searching a CRL for each newly received certificates, since CRLs may get very long. This is seen in section 2.1, on the right column of page 2. However, when reading the rest of this paragraph, one will see the solution for the disadvantages of high cost and CRL length that Applicant notes is stated in Naor. The pertinent portion reads "Kaufman *et al.* [15, Section 7.7.3] suggested reissuing all certificates whenever the CRL grows beyond some limit. In their proposal, certificates are marked by a serial number instead of an expiration date. (Serial numbers are incremented for each issues certificate. Serial numbers are not reused even when all certificates are reissued.) The CRL contains a field indicating the *first valid certificate*. When all certificates are

reissued, the CRL first valid certificate field is updated to contain the serial

number of the first reissued certificate." One can clearly see here an

identification number (serial number) that is compared against a first valid

certificate (revocation number), wherein IDs smaller than the first valid certificate

are invalid/revoked/non-reissued, and IDs equal to or larger than the first valid

certificate are valid. For additionally clarity in this regard, the pertinent portion of

the second edition of the Kaufman book (published in 2002) referred to in Naor is

provided herewith (section 15.4.1.2 corresponding to the first valid certificate

scheme). The 2002 edition is being provided only because the 1995 edition

cannot be located at this time.

Claim Objections

2.   Claims 1, 13, 14, and 16 are objected to because of the following

informalities:

Claim 1 states that the communication control unit is "operable to revoke a

communication with the server apparatus". This appears to mean that the

communication control unit will halt, terminate, or disallow communication with

the server apparatus, as there is no "revoking" of a communication within the

application as originally filed. Clarity is requested so that the meaning of "revoke"

is clear throughout the claims. Claims 13, 14, and 16 have like wording issues.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for

all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described
> as set forth in section 102 of this title, if the differences between the subject matter sought to
> be patented and the prior art are such that the subject matter as a whole would have been
> obvious at the time the invention was made to a person having ordinary skill in the art to which
> said subject matter pertains. Patentability shall not be negatived by the manner in which the
> invention was made.

3.   Claims 1, 3-8, and 11-17 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Vandergeest (U.S. Patent 6,247,127) in view of Naor (Naor et

al., "Certificate Revocation and Certificate Update", January 26, 1998, pp. 1-12).

Regarding Claim 1,

Vandergeest discloses a communication apparatus for

communicating with a server apparatus based on a server

certificate, the communication apparatus comprising:

A revocation number obtainment unit operable to obtain a

revocation data from a repository apparatus storing the revocation

data, the revocation data being a criterion for judging validity of the

server certificate (Column 3, line 66 to Column 4, line 28; and

Column 5, lines 25-49);

A revocation data storage unit operable to store the

revocation data obtained by the revocation data obtainment unit

(Column 3, line 66 to Column 4, line 28; and Column 5, lines 25-

49);

An identification data reading unit operable to read, from the server certificate, identification data that identifies the server certificate (Column 4, line 53 to Column 5, line 49);

A certificate judgment unit operable to judge the validity of the server certificate (Column 4, line 53 to Column 5, line 49); and

A communication control unit operable to establish a communication with the server apparatus when the certificate judgment unit judges the server certificate to be valid, and operable to revoke a communication with the server apparatus when the certificate judgment unit judges the server certificate not to be valid (Column 4, line 53 to Column 5, line 49);

But does not explicitly disclose the use of revocation and identification numbers and comparing such numbers to determine validity of the certificate.

Naor, however, discloses a revocation number obtainment unit operable to obtain a revocation number from a repository apparatus storing the revocation number, the revocation number being a criterion for judging validity of a certificate (Pages 1-2, sections 1-2.1);

An identification number reading unit operable to read, from the certificate, an identification number that identifies the certificate (Pages 1-2, sections 1-2.1); and

A certificate judging unit operable to judge the validity of the certificate by comparing the identification number that identifies the server certificate with the revocation number stored by the revocation number storage unit (Pages 1-2, sections 1-2.1);

Wherein the certificate judgment unit (i) judges whether or not the identification number that identifies the server certificate is smaller than the revocation number stored by the revocation number storage unit, (ii) judges that the server certificate is not valid when the identification number that identifies the sever certificate is judged to be smaller than the revocation number stored by the revocation number storage unit, and (iii) judges that the server certificate is valid when the identification number that identifies the server certificate is judges to be equal to or larger than the revocation number stored by the revocation number storage unit (Pages 1-2, sections 1-2.1). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the CRL management techniques of Naor into the certificate verification system of Vandergeest in order to prevent certificate revocation lists from becoming too large and thus becoming difficult to manage, to provide a simple method of checking validity of certificates, and/or to reduce communication costs related to sending large amounts of data related to certificates and their revocation status.

Regarding Claim 14,

Claim 14 is a method claim that corresponds to apparatus claim 1 and is rejected for the same reasons.

Regarding Claim 16,

Claim 16 is a computer-readable recording medium claim that corresponds to apparatus claim 1 and is rejected for the same reasons.

Regarding Claim 3,

Vandergeest as modified by Naor discloses the apparatus of claim 1, in addition, Vandergeest discloses a revocation data judgment unit operable to judge validity of the revocation data stored by the revocation data storage unit, wherein the certificate judgment unit judges the validity of the server certificate when the revocation data judgment unit judges that the revocation data stored by the revocation data storage unit is valid (Column 4, line 36 to Column 5, line 49); and Naor discloses a revocation number judgment unit operable to judge validity of the revocation number, wherein the certificate judgment unit judges the validity of the certificate when the revocation number judgment unit judges that the revocation number is valid (Pages 1-2, sections 1-2.1).

Regarding Claim 4,

Vandergeest as modified by Naor discloses the apparatus of claim 3, in addition, Vandergeest discloses that the revocation data

judgment unit judges the validity of the revocation data stored by

the revocation data storage unit by comparing identification data of

a repository certificate indicating validity of the repository apparatus

with the revocation data stored by the revocation data storage unit

(Column 4, line 36 to Column 5, line 49); and Naor discloses that

the revocation number judgment unit judges the validity of the

revocation number by comparing an identification number of a

repository certificate indicating validity of the repository apparatus

with the revocation number stored by the revocation number

storage unit (Pages 1-2, sections 1-2.1).

Regarding Claim 5,

Vandergeest as modified by Naor discloses the apparatus of

claim 4, in addition, Naor discloses that the revocation number

judgment unit judges that the repository apparatus is valid when the

identification number of the repository certificate is equal to or

larger than the revocation number stored by the revocation number

storage unit (Pages 1-2, sections 1-2.1).

Regarding Claim 6,

Vandergeest as modified by Naor discloses the apparatus of

claim 3, in addition, Naor discloses that the revocation number

judgment unit judges the validity of the revocation number obtained

by the revocation number obtainment unit by comparing the

revocation number obtained by the revocation number obtainment

unit with the revocation number stored by the revocation number storage unit (Pages 1-2, sections 1-2.1).

Regarding Claim 7,

Vandergeest as modified by Naor discloses the apparatus of claim 6, in addition, Naor discloses that the revocation number judgment unit judges that the revocation number obtained by the revocation number obtainment unit is valid, when the revocation number obtained by the revocation number obtainment unit is equal to or larger than the revocation number stored by the revocation number storage unit (Pages 1-2, sections 1-2.1).

Regarding Claim 8,

Vandergeest discloses a certificate issuing apparatus for issuing a server certificate indicating validity of a server apparatus, the certificate issuing apparatus comprising:

A revocation data storage unit operable to store a revocation data, the revocation data bring a criterion for judging validity of the server certificate (Column 3, lines 25-65);

A revocation data update unit operable to update the revocation data stored by the revocation data storage unit in order to provide for revocation of identification data of server certificates to be revoked (Column 2, lines 1-16; Column 3, lines 25-65; and Column 4, lines 36-52); and

An issuing unit operable to issue a new server certificate (Column 3, lines 25-65);

Wherein the issuing unit issues the new server certificate that includes identification data indicating that the certificate is currently valid (Column 3, lines 25-65);

But does not explicitly disclose that use of revocation and identification numbers and use of such numbers in determining validity of certificates.

Naor, however, discloses a revocation number storage unit operable to store a revocation number being a criterion for judging validity of a server certificate (Pages 1-2, sections 1-2.1);

A revocation number update unit operable to update the revocation number stored by the revocation number storage unit to a number that is larger than an identification number of a server certificate to be revoked, the revocation number update unit updating the revocation number when being notified of the identification number of the server certificate to be revoked (Pages 1-2, sections 1-2.1); and

An issuing unit operable to issue a new certificate including an identification number indicating a value that is equal to or larger than the revocation number stored by the revocation number storage unit (Pages 1-2, sections 1-2.1); and

Wherein, when the revocation number update unit updates the revocation number, the issuing unit issues the new server certificate to another server apparatus that corresponds to a server certificate including an identification number indicating a value that is smaller than the updated revocation number (Pages 1-2, sections 1-2.1). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the CRL management techniques of Naor into the certificate verification system of Vandergeest in order to prevent certificate revocation lists from becoming too large and thus becoming difficult to manage, to provide a simple method of checking validity of certificates, and/or to reduce communication costs related to sending large amounts of data related to certificates and their revocation status.

Regarding Claim 15,

Claim 15 is a method claim that corresponds to apparatus claim 8 and is rejected for the same reasons.

Regarding Claim 17,

Claim 17 is a computer-readable recording medium claim that corresponds to apparatus claim 8 and is rejected for the same reasons.

Regarding Claim 11,

Vandergeest as modified by Naor discloses the apparatus of

claim 8, in addition, Naor discloses an expiration date revocation

number update unit operable to specify an identification number of

a server certificate, specify an approaching expiration date, and

update the revocation number stored by the revocation number

storage unit to a number that is larger than the specified

identification number of the server certificate (Pages 1-2, sections

1-2.1).

Regarding Claim 12,

Vandergeest as modified by Naor discloses the apparatus of

claim 11, in addition, Naor discloses that, when the expiration date

revocation number update unit updates the revocation number

stored by the revocation number storage unit, the issuing unit

issues the new server certificate to a server apparatus with a server

certificate that is assigned an identification number that is smaller

than the revocation number updated by the expiration date

revocation number update unit (Pages 1-2, sections 1-2.1).

Regarding Claim 13,

Claim 13 is a communication system comprising the

certificate issuing apparatus of claim 8, the communication

apparatus of claim 1, and the server apparatus discussed in both

claims 1 and 8, and is therefore rejected for the same reasons as

the combination of claims 1 and 8.

Conclusion

The prior art made of record and not relied upon is considered pertinent to

applicant's disclosure.

Kaufman et al., "Network Security: Private Communication in a Public

World, Second Edition", 4/22/2002, pp. 1-8.

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of

time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire

THREE MONTHS from the mailing date of this action. In the event a first reply is

filed within TWO MONTHS of the mailing date of this final action and the advisory

action is not mailed until after the end of the THREE-MONTH shortened statutory

period, then the shortened statutory period will expire on the date the advisory

action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be

calculated from the mailing date of the advisory action. In no event, however, will

the statutory period for reply expire later than SIX MONTHS from the mailing

date of this final action.

Any inquiry concerning this communication or earlier communications from

the examiner should be directed to JEFFREY D. POPHAM whose telephone

number is (571)272-7215. The examiner can normally be reached on M-F 9:00-

5:30.

If attempts to reach the examiner by telephone are unsuccessful, the

examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The

fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Jeffrey D Popham
Examiner
Art Unit 2437

/Jeffrey D Popham/
Examiner, Art Unit 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437